



9110-9P P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2017-0048]

The Department of Homeland Security, National Protection and Programs Directorate, National Initiative for Cybersecurity Careers and Studies Cybersecurity Training and Education Catalog Collection

AGENCY: National Protection and Programs Directorate (NPPD), Department of Homeland Security (DHS).

ACTION: 60-day notice and request for comments;

Revised Information Collection Request: 1670-0030

SUMMARY: The DHS NPPD Office of Cybersecurity & Communications (CS&C), Cybersecurity Education & Awareness Office (CE&A), National Initiative for Cybersecurity Careers and Studies (NICCS) will submit the following Information Collection Request to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995.

DATES: Comments are encouraged and will be accepted until **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This process is conducted in accordance with 5 CFR part 1320.

ADDRESSES: Comments must be identified by "DHS-2017-0048"

and may be submitted by one of the following methods:

- Federal eRulemaking Portal: <http://www.regulations.gov>.
- E-mail: niccs@hq.dhs.gov. Include the docket number "DHS-2017-0048" in the subject line of the message.
- Mail: Written comments and questions about this Information Collection Request should be forwarded to DHS/NPPD 245 Murray Lane SW, Mailstop 0380, Arlington, VA 20598-0380.

Instructions: All submissions received must include the words "Department of Homeland Security" and docket number "DHS-2017-0048". Comments received will be posted without alteration at <http://www.regulations.gov>, including any personal information provided. Written comments should reach the contact person listed no later than [***INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER***].

FOR FUTHER INFORMATION CONTACT: For specific questions related to collection activities, please contact Shannon Nguyen at 703-705-6246 or at niccs@hq.dhs.gov.

SUPPLEMENTARY INFORMATION: Title II of the Homeland Security Act of 2002, 6 U.S.C. 121(d)(1), says that the Secretary of Homeland Security has the responsibility "To access, receive, and analyze laws enforcement information, intelligence information and other information from

agencies of the Federal Government, State and local government agencies and Private sector entities and to integrate such information in support of the mission responsibilities of the Department.” The following authorities also permit DHS to collect information of the type contemplated: Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. 3546; Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection (2003); and National Security Presidential Directive (NSPD)-54/HSPD-23, Cybersecurity Policy (2009).

The NICCS Portal is a national online resource for cybersecurity awareness, education, talent management, and professional development and training. NICCS Portal is an implementation tool for NICE. Its mission is to provide comprehensive cybersecurity resources to the public. To promote cybersecurity education, and to provide a comprehensive resource for the Nation, NICE developed the Cybersecurity Training and Education Catalog. The Cybersecurity Training and Education Catalog will be hosted on the NICCS Portal. Training course and certification information will be included in the Training/Workforce Development Catalog.

Any information received from the public in support of the

NICCS Portal and Cybersecurity Training and Education Catalog is completely voluntary. Organizations and individuals who do not provide information can still utilize the NICCS Portal and Cybersecurity Training and Education Catalog without restriction or penalty. An organization or individual who wants their information removed from the NICCS Portal and/or Cybersecurity Training and Education Catalog can e-mail the NICCS Supervisory Office.

CE&A uses the collected information from the NICCS Cybersecurity Training Course Form and the NICCS Cybersecurity Certification Form and displays it on a publicly accessible website called the National Initiative for Cybersecurity Careers and Studies (NICCS) Portal (<http://niccs.us-cert.gov/>). Collected information from these two forms will be included in the Cybersecurity Training and Education Catalog that is hosted on the NICCS Portal.

The DHS CE&A NICCS Supervisory Office will use information collected from the NICCS Vendor Vetting Form to primarily manage communications with the training/workforce development providers; this collected information will not be shared with the public and is intended for internal use only. Additionally, this information will be used to

validate training providers before uploading their training and certification information to the Training Catalog.

The DHS CE&A NICCS Supervisory Office will use information collected from the NICCS Mapping Tool Form to provide an end user with information of how their position or job title aligns to the new Cybersecurity Framework 1.1. This collected information will not be shared with the public and is intended for internal use only.

The information will be collected via fully electronic web forms or partially electronic via email. Collection will be coordinated between the public and DHS CE&A via e-mail (niccs@hq.dhs.gov).

The revisions to the collection include: the addition of the NICCS Mapping Tool, the updates to the Training Course Form, Changing a form name from Vetting Criteria Form to Vendor Vetting Form, Course Certification Form has been updated to be collected via email as a CSV file.

OMB is particularly interested in comments that:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
2. Evaluate the accuracy of the agency's estimate of

the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

3. Enhance the quality, utility, and clarity of the information to be collected; and
4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

Title: National Initiative for Cybersecurity Careers and
Studies Cybersecurity Training and Education Catalog
Collection

OMB Number: 1670-0030

Frequency: Occassionally

Affected Public: Educational Institutes (Privately Owned,
and State/Local Government Owned)

Number of Respondents: 1,350 respondents

Estimated Time per Respondent: 30 minutes

Total Burden Hours: 1,688 annual burden hours

Total Burden Cost: \$0

Total Recordkeeping Burden: \$0

Scott Libby,
Deputy Chief Information Officer.

[FR Doc. 2017-25102 Filed: 11/17/2017 8:45 am; Publication Date: 11/20/2017]